What is claimed is:

1. A method wherein users are assigned a data key for at least one of encrypting and decrypting data, comprising:

performing a security check to ascertain an identity of a user;

assigning a data key, unviewable by the user, on the basis of a result of the security check, wherein the same data key is assignable to a plurality of users.

2. The method as claimed in claim 1, wherein the security check involves checking biometric data of the user.

3. The method as claimed in claim 1, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

4. The method as claimed in claim 1, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

5. The method as claimed in claim 4, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

6. The method as claimed in claim 1, wherein a plurality of data keys are simultaneously assignable to one user.

7. The method as claimed in claim 1, wherein the data are medically relevant, wherein the users include

personnel at a medical facility, and wherein common user groups are assigned the same data key.

8. An electronic data processing facility for at least one of encryption and decryption of data, wherein a data key for encrypting and decrypting data is assignable to a user, comprising:

security check means for performing a security check to ascertain an identity of the user; and

means for assigning a data key, unviewable by the user, on the basis of a result of the security check, wherein the same data key is assignable to various users.

9. The electronic data processing facility as claimed in claim 8, wherein the security check means is for checking biometric data from the user.

10. The electronic data processing facility as claimed in claim 8, wherein the security check means is for checking a user-specific at least one of electronic and mechanical key.

11. The electronic data processing facility as claimed in claim 9, wherein a data key memory is accessible by the data processing facility, for ascertaining the data key assigned by comparing the data obtained through the security check with the content of the data key memory.

12. The electronic data processing facility as claimed in claim 11, wherein the data key memory is arranged remotely from the data processing facility, and wherein the data processing facility uses a data telecommunication device to access the data key memory.

13. The electronic data processing facility as claimed in claim 8, wherein the data processing facility is a medical workstation for handling medically relevant data.

14. A storage medium, adapted to store information and adapted to interact with a data processing facility in order to carry out the method as claimed in claim 1.

15. The method as claimed in claim 2, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

16. The method as claimed in claim 2, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

17. The method as claimed in claim 3, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

18. The method as claimed in claim 16, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

19. The method as claimed in claim 17, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

20. The electronic data processing facility as claimed in claim 9, wherein the security check means is for checking a user-specific at least one of electronic and mechanical key.

21. The electronic data processing facility as claimed in claim 10, wherein a data key memory is accessible by the data processing facility, for ascertaining the data key assigned by comparing the data obtained through the security check with the content of the data key memory.

22. A method for at least one of encryption and decryption of data, comprising:

assigning a user a data key for at least one of encrypting and decrypting data;

performing a security check to ascertain an identity of a user, wherein a data key, unviewable by the user, is assigned on the basis of a result of the security check, and wherein the same data key is assignable to a plurality of users.

23. A storage medium, adapted to store information and adapted to interact with a data processing facility in order to carry out the method as claimed in claim 22.

24. The method as claimed in claim 22, wherein the security check involves checking biometric data of the user.

25. The method as claimed in claim 22, wherein the security check involves checking a user-specific at least one of electronic and mechanical key.

26. The method as claimed in claim 22, wherein the data key is ascertained by comparing the data obtained in the security check with content of a data key memory.

27. The method as claimed in claim 26, wherein the data obtained in the security check are compared with the content of the data key memory using a data telecommunication device.

28. The method as claimed in claim 22, wherein a plurality of data keys are simultaneously assignable to one user.

29. The method as claimed in claim 22, wherein the data are medically relevant, wherein the users include personnel at a medical facility, and wherein common user groups are assigned the same data key.

30. The method of claim 22, wherein users associated with a common user group are assigned the same data key.

31. An electronic data processing facility for at least one of encryption and decryption of data, comprising:

means for assigning a user a data key for at least one of encrypting and decrypting data;

means for performing a security check to ascertain an identity of a user, wherein a data key, unviewable by the user, is assignable on the basis of a result of the security check, and wherein the same data key is assignable to a plurality of users.

32. The method of claim 1, wherein users associated with a common user group are assigned the same data key.